

Policy for Processing of Personal Data

January 2025

Table of content

1. Introduction	3
2. Roles and Responsibilities	3
3. Definitions.....	4
4. Scope and Limitations	4
5. Processing of Personal Data	4
6. Data Protection in DLR	4
7. Rights of Data Subjects.....	5
8. DLR's Obligations.....	5

1. Introduction

This policy is based on the provisions of the EU General Data Protection Regulation (GDPR), which applies in the EU and governs the processing of personal data relating to DLR's customers and employees. DLR must also adhere to the supplementary Data Protection Act.

The purpose of this policy is to outline the decisions and measures DLR must follow as a foundation for processing various types of personal data.

The policy begins with a description of internal responsibilities at DLR and is structured according to the initial chapters of the GDPR, namely:

- Scope and Limitations
- Processing of Personal Data
- Principles
- Rights of Data Subjects
- DLR's Obligations
- Special Considerations

2. Roles and Responsibilities

The board and management are responsible for this policy for processing personal data at DLR.

The Data Protection Officer (DPO) is responsible for supporting DLR in complying with the GDPR. Specific obligations are outlined in the section "DLR's Obligations."

DLR's Project Manager and Chief Legal Officer are designated as GDPR officers, responsible for ensuring the implementation and adherence to this policy across the organization on behalf of management.

The Legal and Regulatory department is responsible for legal assessments related to GDPR and the implications of national interpretations for DLR.

Department managers must ensure the policy's requirements, as set out in business procedure "G34", are met within their respective areas.

External partners and their employees must, through agreements, be required to process personal data for which DLR is responsible in accordance with DLR agreements, including data processing agreements.

3. Definitions

Term	Definitions
Processing:	Includes activities such as collection, registration, organization, systematization, storage, adaptation or alteration, retrieval, search, use, disclosure by transmission, dissemination or any other form of transfer, alignment or combination, restriction, deletion, or destruction.
Personal Data:	<p>Personal data refers to any form of information about an identifiable natural person.</p> <p>Personal data is divided into two categories:</p> <ul style="list-style-type: none"> • Sensitive personal data includes race or ethnic origin, political, religious, or philosophical beliefs, trade union membership, genetic data, biometric data, health information, or data concerning a natural person's sexual orientation as well as information about criminal matters. • General personal data includes all other information about a person, such as name, address, email, telephone/mobile number, date of birth, marital status, education, examinations, employment matters, housing, car, finances, salary, taxes, IP address, behavior, purchases, location, etc., as well as social security numbers or other national identification numbers.

4. Scope and Limitations

This policy outlines requirements for all forms of personal data processing conducted by DLR for customers and employees.

Detailed requirements are elaborated in business procedure G34 and are implemented in departmental procedures.

5. Processing of Personal Data

A record of processing activities must be prepared, documenting the categories of personal data that DLR processes in the various IT systems.

6. Data Protection in DLR

DLR's activities require the handling of personal data. The majority of the data consists of general personal data; however, some of this is confidential information, which must not be disclosed to unauthorized people or the public. Of the personal data DLR processes, the majority concerns customers and partners, while only a small portion relates to employees and other groups.

DLR processes sensitive personal data only to a limited extent, which is almost exclusively related to employee information.

DLR places great emphasis on ensuring that the processing of personal data complies with the rules set forth in GDPR and the supplementary Data Protection Act.

7. Rights of Data Subjects

DLR's processes, IT systems, and data processing agreements must ensure that customers, partners, and employees can exercise their rights under GDPR, including:

- **Right of Access:** Individuals have the right to know what personal data DLR processes about them.
- **Right to Rectification:** Individuals can request correction of incorrect data without undue delay.
- **Right to Erasure:** Individuals can request deletion of personal data under specific conditions.
- **Right to Withdraw Consent:** Individuals can withdraw their consent at any time.
- **Right to Restriction:** Individuals can request limited data processing under certain conditions.
- **Right to Data Portability:** Individuals can request their data in an electronic format under certain circumstances.

8. DLR's Obligations

DLR has conducted a risk assessment concerning the data subjects, which describes the risk landscape associated with the registered personal data.

The business procedure for the organization, management, and oversight of IT security at DLR (I2) and the Contingency Plan for handling breaches of personal data security cover the handling of security breaches concerning DLR's registered personal data, including reporting such incidents to the Data Protection Authority.

DLR's Data Protection Officer (DPO) is responsible for ensuring that the following tasks are carried out:

- **Notification and Guidance**
Providing notifications and guidance to DLR's management and employees who process personal data on their obligations under the regulation.

There may periodically be a need to conduct "brush-up" sessions to refresh employees' knowledge.
- **Monitoring**
Ensuring compliance with the regulation's requirements within DLR, including DLR's policies related to data protection.

Contact Point between Public Authorities and DLR

The DPO acts as the primary contact point between supervisory authorities and DLR regarding data protection and personal data processing and must collaborate with the Data Protection Authority.

In the event of a personal data breach, the DPO is also responsible for notifying authorities about the breach, its circumstances, and measures to prevent similar breaches in the future.

Reporting to the Board

The DPO reports to the board as needed, but at least annually, regarding DLR's handling of data protection matters.

This "Policy for Processing of Personal Data" was translated in January 2025 and is based on "Politik for behandling af personoplysninger" approved by the board of directors of DLR Kredit A/S at its meeting on October 30, 2023.